Attorney Docket No.: LYRN004US0

PATENTS
Customer No. 37,141

REMARKS:

Claims 1-22 are currently pending in the application, and have been rejected.

Prior to addressing each of the Examiner's grounds of rejection individually, the Examiner is respectfully reminded that it is insufficient for the purposes of establishing a prima facie case of obviousness to merely find a collection of prior art references which, collectively, disclose each of the individual elements of a claimed invention. Rather, the Examiner must provide proper incentive for one skilled in the art to combine the references in the manner suggested by the Examiner so as to arrive at the claimed invention. In doing so, the Examiner may not pick and choose among the teachings of a reference. Rather, each reference must be construed as a whole for what it fairly suggests to one skilled in the art. Moreover, in construing the references, the use of hindsight must be avoided.

Reconsideration of the Examiner's rejection of claims 1-6 and 19-21 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 6,560,450 (Rosenberg et al.) in view of U.S. 6,687,732 (Bector et al.) is respectfully requested.

In their previous response, Applicants noted that the present claims require, in essence, that the message is routed to the "next location" regardless of whether the message is in the selected application format, since the only effect of the application format is whether the message is processed by the selected application processor. Applicants also noted that it is clear that the "next location" referred to in the claims is the same in each instance, because the first instance of this element is "routing the message to a next location", and the second instance of this element is "routing the message to the next location" [emphasis added]. By contrast, Applicants noted that, in the system of Rosenberg et al., the "next location" that the message is sent to necessarily differs depending on the outcome of the Gray code analysis. In particular, if the Gray code analysis reveals a match, the message is sent to the ground station serviced by the satellite and on to its destination,

whereas if the Gray code analysis reveals no match, the message is sent to another satellite in the network.

To the extent that Applicants can understand the Examiner's reply to their arguments, the Examiner appears to agree that Rosenberg et al. fails to teach a system in which a packet is routed to the same "next location" irregardless of whether it is in the selected application format. However, the Examiner relies on Bector et al. for this teaching.

Applicants respectfully note, however, that the Examiner has not provided sufficient incentive for combining the teachings of Bector et al. with those of Rosenberg et al. as required to arrive at the claimed invention. In particular, the satellite nodes in the system of Rosenberg et al. are transmission nodes in that network. By contrast, the device Bector et al. is concerned with is a proxy server. See FIG. 1 thereof. The Examiner has not established that one skilled in the art would have any incentive to replace any of the satellite nodes in the system of Rosenberg et al. with a proxy server, or even with the functionality required to intercept packages and determine whether they should be sent to a proxy server.

To the contrary, when Rosenberg et al. is construed as a whole for what it fairly suggests to one skilled in the art, it is clear that the reference was concerned with developing a simplified routing scheme which would require storing as little information in the satellite as possible. In this respect, it is to be noted that the reference expounds, at Col. 2, Lines 5-22, on the cost and undesirability of storing information at the satellite level, and notes, at Col. 4, Lines 10-14, that the methodology disclosed therein "provides a routing strategy that is simple, robust, efficient, that does not require a large amount of information to be stored in the satellite and does not require a large number of exchanges of information between satellites." [emphasis added]. Hence, the solution proposed by Rosenberg et al. is a simplified routing scheme which eases the computational burden imposed by the routing function.

The modification to Rosenberg et al. which is proposed by the Examiner (namely, the incorporation of a proxy server of Bector et al. into the system of Rosenberg et al. or the additional routing functionality required to work in conjunction with that proxy server) would defeat the very purpose of Rosenberg et al. by significantly complicating the functionality of the satellite node. This would require additional computational assets in space, something Rosenberg et al. clearly

teaches away from. For the sake of completeness, Applicants note that, while it may be possible to incorporate the methodology of Bector et al. into the ground-based portion of Rosenberg et al., the Examiner's analysis is not based on this possibility, nor would such a modification of Rosenberg et al. lead to the invention as claimed.

Regarding claim 6, Applicants note that this claim requires, in essence, that the "selected application format" is the encryption state of the message. The Examiner argues that Rosenberg et al. teaches that the message is encrypted, and further teaches that processing the message by the selected application processor includes decrypting the message by the selected application processor. Here, the Examiner cites Col. 5, lines 54-58 of Rosenberg et al. in support of his assertion.

However, the cited portion of Rosenberg et al. describes only encoding and decoding of data which occurs at the terminals at the edge of the satellite network, and hence not at the satellite nodes themselves. Thus, the application processor cannot be a satellite node, but must be an edge terminal. If that is so, however, the "next location" also cannot be a satellite node, since then the edge terminal would be transmitting unencrypted data to a satellite node where it could be intercepted and understood by an eavesdropper. One skilled in the art would have no incentive for transmitting unencrypted data in this manner, since the fact that the data was originally encrypted indicates that security of the data is a concern. Hence, the Examiner's rejection would have to be rooted solely on the ground-based portion of the system of Rosenberg et al., which is not in keeping with the manner in which the Examiner has applied the reference.

Moreover, the Examiner's contention that the "selected application format" is the encryption state of the message is at odds with his grounds of rejection for claim 1, where the Examiner argues that the selected application format was the package header incorporating a destination address. Since claim 6 depends from claim 1, the Examiner cannot have it both ways. Hence, claim 6 would be allowable over the cited art, even if the Examiner were correct in his interpretation of that art as it pertains to claim 1.

Regarding claims 19, 20 and 21, the Examiner argues that these claims "are apparatus claims of claims 1, 2 and 6, therefore, they are rejected for the same reasons as claims 1, 2 and 6 above." However, Applicants respectfully note that, contrary to the Examiner's assertion, these

claims are method claims, not apparatus claims. Moreover, claim 19 (from which claims 20 and 21 depend) recites limitations not found in claim 1.

Reconsideration of the Examiner's rejection of claims 7-12, 14 and 16-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 6,560,450 (Rosenberg et al.) in view of U.S. 6,687,732 (Bector et al.), and further in view of U.S. 6,578,147 (Shanklin et al.), is respectfully requested.

The Examiner is respectfully reminded that, in order to establish a prima facie case of obviousness based on a proposed combination of references, it is insufficient to merely find each element of the claimed invention within one or more of the cited references. Rather, the Examiner must show how the references, when taken together, would teach or suggest combining and modifying the individual teachings of the references so as to arrive at the claimed invention. The cited references must also teach or suggest the desirability of the proposed modification.

In the present case, the Examiner relies on Rosenberg et al. as the primary reference, and relies on Bector et al. and Shanklin et al. as secondary references. Hence, whenever Rosenberg et al. fails to teach an element of the claimed invention, the Examiner must show how one of the secondary references teaches the missing element, and must also explain how the secondary reference teaches or suggests modifying the system of Rosenberg et al. so as to arrive at the claimed invention.

In the present case, the Examiner concedes that neither Rosenberg et al. nor Bector et al. teach processing a message in parallel, but relies upon Shanklin et al. for this teaching. In particular, the Examiner notes in essence that Shanklin et al. teaches that the sensors disclosed therein operate in parallel to determine "if any packet or series of packets has a "signature" that matches one of a collection of known intrusion signatures" [here Applicants are quoting the cited portion of Shanklin, and not the Examiner per se].

However, even if the Examiner's construction of Shanklin et al. is assumed to be correct, when Shanklin et al. is construed as a whole for what it fairly suggests to one skilled in the art, the reference simply does not teach or suggest the modification of Rosenberg et al. as required to arrive at the claimed invention. To the contrary, it is quite clear that the above noted "parallel processing"

which occurs in Shanklin et al. occurs at the entry point to the network. Thus, Col. 2, lines 48-50 of Shanklin et al. state that

> Multiple intrusion detection sensors are used at the entry point to the network, specifically, at an "internetworking device" such as a router or switch. These devices have in common the function of linking a local network to an external network, such as another local network or to a wide area network using a telecommunications link. [emphasis added]

However, claim 7 clearly requires that "the plurality of application specific service devices are further configured to process the unprocessed application-specific messages in parallel", and the Examiner has construed the satellite nodes of Rosenberg et al. as being the "plurality of application service devices". Hence, in order to support a prima facie case of obviousness, Shanklin et al. must teach or suggest modifying the system of Rosenberg et al. so that the satellite nodes described therein utilize the parallel processing methodology of Shanklin et al.

Unfortunately for the Examiner, Shanklin et al. does not contain any such teaching or suggestion. To the contrary, as noted above, Shanklin et al. clearly teaches that the methodology taught therein should be applied to the entry point of a network. Indeed, this point is underscored by the drawings in Shanklin et al., which depict the sensors which implement that methodology as being disposed proximal to the router (see, e.g., FIG. 1), and by the claims, which recite the intrusion detector sensors as being disposed between a router and a local network (see, e.g., claim 1, Lines 4-5).

The satellite nodes in Rosenberg et al. are clearly not entry points to the network disclosed therein, but rather, are intermediate points within that network. Hence, Shanklin et al. clearly does not teach or suggest applying the methodology taught therein to the satellite nodes of Rosenberg et al. Indeed, it would make no sense to apply the methodology of Shanklin et al. to the satellite nodes of Rosenberg et al., since the stated purpose of the methodology of Shanklin et al. is to provide intrusion detection so that unauthorized access to a network may be prevented. By the time a packet reaches a satellite node in the system of Rosenberg et al., the network has already been accessed. Hence, the proposed modification of Rosenberg et al. would be undesirable.

With respect to claim 10, the Examiner argues that Shanklin et al. "teaches the plurality of application service devices is included in a single integrated circuit". Applicants respectfully note

that this interpretation is inconsistent with the Examiner's argument in the rejection of the base claim that the plurality of application service devices are satellite nodes. A similar observation may be made with respect to claims 11.

Regarding claim 14, the Examiner points to Col. 5, Lines 56-61 of the application as teaching an unprocessed application stream. Apparently, the Examiner is interpreting a packet that has not passed through the intrusion detection sensors as being the "unprocessed application stream" required by claim 14.

However, claim 14 depends from claim 7, which requires that the application service devices process the unprocessed application-specific messages in parallel. As previously noted, the Examiner has interpreted the application service devices as being the satellite nodes (element 11 in Rosenberg et al.). By contrast, the intrusion detection sensors in the portion of Shanklin et al. cited by the Examiner are clearly incorporated into a router. Hence, even if the packets that have not passed through the intrusion detection sensors of Shanklin et al. could be construed as an "unprocessed application stream" as required by claim 14, the Examiner has failed to explain how this teaching would lead one skilled in the art to modify the satellite nodes in Rosenberg et al. so as to arrive at the claimed invention.

With respect to claim 18, the Examiner contends that Col. 5, Lines 63-64 of Shanklin et al. teaches a TPC offload engine communication. However, Applicants respectfully note that the cited portion of Shanklin does not contain the teachings the Examiner is ascribing to it. Rather, this portion of the reference merely teaches the concept of implementing packet-based load balancing through sensor redundancy.

Reconsideration of the Examiner's rejection of claim 13 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 6,560,450 (Rosenberg et al.) in view of U.S. 6,687,732 (Bector et al.) and U.S. 6,578,147 (Shanklin et al.), and further in view of Troubleshooting (TB), is respectfully requested.

The infirmities of Rosenberg et al., Bector et al. and Shanklin et al. have been noted above with respect to claim 7, from which claim 13 depends. These infirmities are not cured by TB, nor was TB cited for that purpose. Hence, claim 13 is allowable for the same reasons as claim 7.

Moreover, Applicants respectfully note that claim 13 requires that "one of the plurality of application service devices comprises as SSL/TLS processor". Since the Examiner has interpreted the satellite nodes of Rosenberg et al. as being the "plurality of application service devices" set forth in claim 7, this interpretation requires that one of the satellite nodes in the system of Rosenberg et al. must comprise an SSL/TLS processor. However, the Examiner has failed to provide sufficient incentive for one skilled in the art to modify the system of Rosenberg et al. in this manner.

As a preliminary matter, Applicants respectfully note that TB is merely a troubleshooting guide which, by its own description set forth in the first page of the reference, "provides a list of common errors, their meanings, and possible solutions". As such, although the reference mentions SSL/TLS in the context of error messages, contrary to the Examiner's insinuation, TB is devoid of any teaching or suggestion that SSL/TLS is desirable for implementing encryption acceleration hardware, or that a system of the type disclosed in Rosenberg et al. should be modified to implement SSL/TLS. While Applicants candidly admit that SSL/TLS is a protocol which is, by itself, well known in the art, that fact simply does not suggest modifying the satellite nodes of Rosenberg et al. with an SSL/TLS processor as would be necessary to support a prima facie case of obviousness under the Examiner's analysis.

SSL/TLS refers to the RSA public-key cryptographic operations usually used to exchange the session key at the start of a connection. It is well known in the art that these operations are computationally intensive, and that it typically takes far more CPU time to establish an SSL connection than a normal connection. One skilled in the art would have no incentive to modify the satellite nodes in the system of Rosenberg et al. to implement SSL/TLS, because the messages transmitted to a satellite node in that system would already be encrypted. Indeed, Rosenberg et al. teaches as much at Col. 5, lines 54-58. Were this not the case, the whole system of Rosenberg et al. would be insecure, since an eavesdropper could readily intercept and understand any message being

transmitted from a ground station to the satellite node. Hence, modifying the satellite nodes in the system of Rosenberg et al. to implement SSL/TLS would constitute a useless redundancy.

Such a modification would be further undesirable in that the substantial computational cost attendant to the modification would greatly slow down the entire network, and would require the placement of substantially greater computational assets in space. Given the substantial cost of assets in space and the difficulty of maintaining those assets, one skilled in the art would have no incentive to modify the system of Rosenberg et al. in this manner. Rather, if it was desired to implement an SSL/TLS protocol in such a system, it would be implemented on the ground, and likely at a router or other such device placed close to the client or to the server.

Reconsideration of the Examiner's rejection of claim 15 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 6,560,450 (Rosenberg et al.) in view of U.S. 6,687,732 (Bector et al.) and U.S. 6,578,147 (Shanklin et al.), and further in view of Troubleshooting (TB), is respectfully requested.

Applicants respectfully note that claim 15 requires that the application streams comprise an SSL/TLS connection between a web browser and a web server. However, through its dependencies claim 15 also requires, in essence, that the processed application stream be processed by an application service device, which the Examiner has construed to be the satellite nodes in the system of Rosenberg et al. As noted above with respect to claim 13, the cited art neither teaches nor suggests processing SSL/TLS protocols at the satellite nodes of Rosenberg et al., nor would one skilled in the art have incentive to do so. It is thus respectfully submitted that the Examiner has failed to establish a prima facie case of obviousness with respect to claim 15.

Reconsideration of the Examiner's rejection of claim 22 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 6,560,450 (Rosenberg et al.) in view of U.S. 6,687,732 (Bector et al.), and further in view of U.S. 6,820,250 (Muthukumar et al.), is respectfully requested.

Attorney Docket No.: LYRN004US0

PATENTS
Customer No. 37,141

The infirmities of Rosenberg et al. and Bector et al. are noted above. These infirmities are not cured by Muthukumar et al. Indeed, Muthukumar et al. was cited solely for its teachings regarding software pipelining. It is thus respectfully submitted that claim 22 is allowable for reasons noted above.

It is believed that no fees are due with this response. However, if any fees are due, the Commissioner is hereby authorized to charge these fees, or to credit any overpayment, to the deposit account of Fortkort & Houston, Deposit Account No. 50-3694. Please reference our Docket No. LYRN004US0.

Respectfully submitted,

FORTKORT & HOUSTON P.C.

Dated: January 29, 2007

By: _____
John A. Fortkort
Reg. No. 38,454

9442 N. Capital of Texas Hwy
Arboretum Plaza One; Suite 500
Austin, Texas 78759
Telephone: (512) 343-4525
Facsimile: (512) 343-4530
jfortkort@foholaw.com